AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

FILED

OCT 30 2019

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

In the Matter of the Search of

The residence located at 1545 Hollywood Ln, Florissant, MO 63033, further described as a single story building with brick and wood siding, white trim, and the numbers "1545" displayed diagonally just left of the front door.

Case No. 4:19 MJ 7417 SPM

APPLICATION FOR A SEARCH WARRANT

I, Peter Dyer, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the EASTERN District of MISSOURI, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 1341	Mail Fraud
18 USC 1343	Wire Fraud

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Peter Dyer, United States Postal Inspector

Printed name and title

Sworn to before me and signed in my presence.

Date: 10.30.2019

Judge's signature

City and state: St. Louis, MO

Honorable Shirley Padmore Mensah, U.S. Magistrate Judge

Printed name and title

AUSA: Tracy L. Berry

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF: The residence located at 1545 Hollywood Lane, Florissant, MO 63033, further described as a single story building with brick and wood siding, white trim, and the numbers "1545" displayed diagonally just left of the front door.	Case No. 4:19 MJ 7417 SPM **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT

I, Peter Dyer, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Postal Inspector with the U.S. Postal Inspection Service ("USPIS") and have reason to believe that on and within the property known as: **1545 Hollywood Lane, Florissant, MO 63033 (Further described in Attachment A),** which is located within St. Louis, Missouri, in the Eastern District of Missouri, there is now concealed items, namely: **The items listed in "Attachment B, Items to be Seized,"** which constitutes evidence of the commission of a criminal offense or which is contraband, fruits of the crime, or things otherwise criminally possessed, or which is designed or intended for use or which is or has been used as the means of an offense, in violation of Title 18, United States Code, Section 1341, Mail Fraud; Title 18 United States Code, Section 1343, Wire Fraud, Title 18, United States Code, Section 1028A, Aggravated Identity Theft, and other violations. The facts to support the issuance of a Search Warrant are as follows:

2. I am a Postal Inspector with USPIS and have been so employed since August 2019. I primarily work complex financial fraud investigations that involve the United States Mail system. I have been trained in the investigation of mail fraud and related crimes. Prior to my current appointment, I was employed as a Special Agent with the United States Department of Treasury, Internal Revenue Service, Criminal Investigation for eight years where I worked complex financial fraud investigations. Over the past two years I was also assigned to the FBI's Cyber Task Force where I investigated offenses relating to the criminal use of technology including the criminal use

of computers and computer networks in the commission of fraud schemes. I have participated in numerous investigations into criminal violations of the United States Code including numerous Wire Fraud cases like the one described in this affidavit.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. I have not set forth each and every fact known to me concerning this investigation. I have included what I believe are facts sufficient for the present purpose.

4. The information contained in this affidavit is based upon my personal knowledge as well as information conveyed to me by other law enforcement agents and employees, and what I have learned from other sources specifically detailed herein.

TRAINING AN EXPERIENCE OF THE INVESTIGATIVE TEAM

5. Based on your affiant's knowledge, training, an experience, and the knowledge, training and experience of the investigative team, your affiant knows that:

a. Fraud schemes that use artificial romantic intentions towards a victim, gaining their affection, and then use that goodwill to direct the victim to send money or conduct financial transactions on scammer's behalf, are known as Romance Scams.

b. Romance scams lure victims by creating and using fictitious online dating profiles and social media accounts using aliases and stolen photographs. Scammers claim to be in the military or working overseas, which explains why they cannot meet in person.

c. After grooming their victims, scammers create fictional scenarios alleging a financial hardship and ask the victim to send money to the scammer and/or conduct financial transactions on their behalf. Travel costs, airfare to meet the victims, and income tax liabilities are frequently used scenarios to solicit money from the victims.

d. Romance scammers enlist others to participate in various roles to avoid detection by law enforcement. An individual can have one role or many roles depending on the scheme. One such role, the "*mule*", is a person who engages in financial transactions to receive, withdrawal, transfer, or mail proceeds of the scam to others. A mule can be a witting participate or a victim used to funnel proceeds to another mule.

e. Fraudsters often use romance scam victims to unwittingly conduct transactions using financial proceeds of other fraud schemes such as business email compromises,

account takeovers, ransomware, or identity theft, in order to avoid law enforcement detection and put layers between themselves and the proceeds.

f. Due to the inherent anonymity of non-traditional banking products such as pre-paid debit cards, reloadable and non-reloadable point-of-sale cards, virtual currency transactions, and peer-to-peer financial applications, it is common for scammers to direct criminal proceeds to these monetary instruments and networks.

g. Due to the inherent anonymity of, and inability to track, United States currency as it is transferred from person to person, it is common for scammers to direct victims to conduct financial transactions in cash.

h. Romance scammers often use multiple computers, cell phones, tablets, and other electronic devices to communicate with others involved in the scheme, initiate and confirm the transfer of stolen funds, track packages sent through the United States Mail, and communicate with each other across the United States and internationally.

i. Romance scammers often use multiple aliases, email addresses, usernames, log-in credentials, and other unique identifiers in order to communicate with scheme participants, conceal their true identity, and avoid detection by law enforcement.

j. Due to the prevalence of electronic communications and storage, paper records can be converted and stored electronically. As a result, any record or document could be found in either paper or electronic format.

PROBABLE CAUSE

6. In October 2019, the USPIS was contacted by the family of "R.A.", a resident of the Eastern District of Wisconsin, to report that he had fallen victim to a scam in which R.A. mailed approximately $140,000 in United States currency to **312 Tacoma Drive, St. Louis, Missouri 63125** (hereinafter referred to as "**312 Tacoma Drive**") and other addresses.

7. In October 2019, your affiant contacted "D.A.", the adult son of R.A, and learned that R.A. was an eighty-two year old United States Military Veteran who sent his entire retirement savings to an individual he believed to be a romantic interest.

8. In May 2019, D.A. learned from R.A. that he was sending money to someone he met online. D.A. became suspicious and, with R.A.'s consent, reviewed R.A.'s electronic communications. These represented communications stored on R.A.'s cell phone and tablet computer.

9. According to R.A.'s electronic communications between May 2018 and September 2019:

a. R.A. met an individual who purported to be a female named R.O. on an online dating website. R.O. claimed to be seeking a romantic relationship with R.A., but was working overseas.

b. R.O. directed R.A. to move their conversation off the dating website and onto Google Hangouts, a mobile device application. R.O. and R.A. also communicated through email and text message.

c. R.O. and R.A. never met in person or participated in internet conversations through FaceTime or Skype.

d. R.O. directed R.A. to send money to her so she could return to the United States and they could continue their relationship. R.O. claimed the money would be used for various purposes such as passport costs, plane tickets, and other travel related costs.

e. R.O. directed R.A. to mail her cash and gift cards, wire funds to her Hong Kong account, and deposit cash into R.O.'s Bitcoin wallet address through a Bitcoin automated teller machine.

f. For the cash transactions, R.O. directed R.A. to withdraw cash from his bank accounts, place the cash inside a book, and send it using the United States Mail and/or FedEx to one of R.O.'s associates at **312 Tacoma Drive**. R.O. claimed the associate would then get the money to her.

10. D.A. obtained the permission of R.A. to research R.A.'s relationship with R.O. and the funds that he provided to her. Subject to R.A.'s consent, D.A. shared with your affiant more than two-hundred screenshot photographs of Google Hangout conversations between R.O. and R.A. which took place between May 30, 2019 and June 27, 2019 as well as images of items D.A. discovered in R.A.'s home.

11. The images of the Google Hangout conversations showed in part the following:

a. On Monday, June 24, 2019, R.O., whose text appears on the left, and R.A., whose text appears on the right, have two separate conservations in which they discuss how to send U.S. currency. See below, Figure 1 and Figure 2.

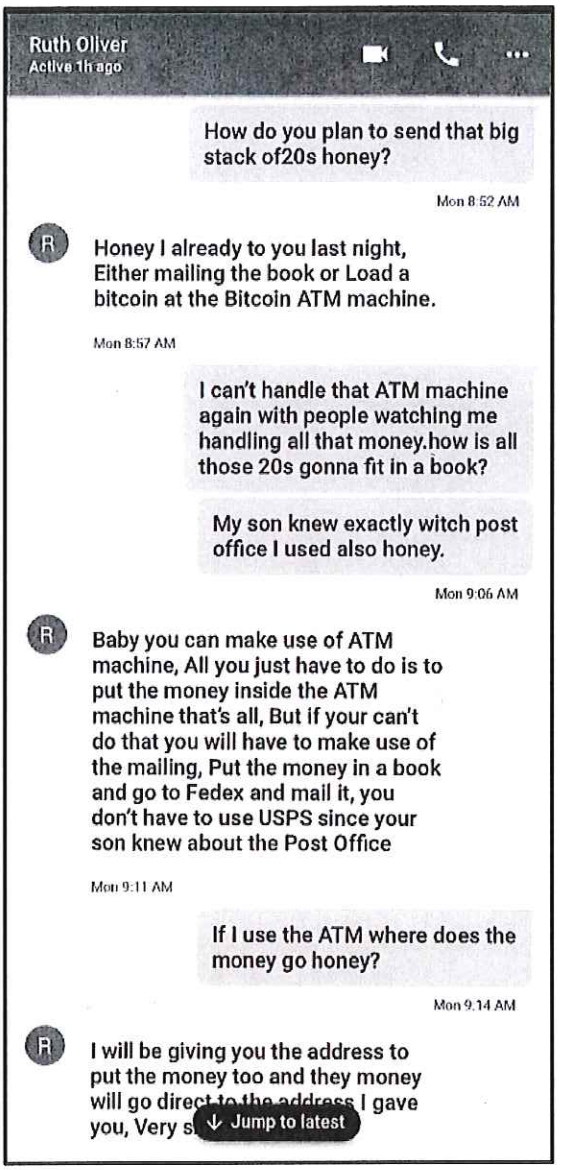

Figure 1

Figure 2

12. D.A. provided your affiant a photograph from R.A.'s electronic device which identified the email address MYPETTWOFACE57@GMAIL.COM and phone number 501-242-5332 as being associated with R.O. This same photograph also identifies R.O.'s Google Hangout account as being associated with phone number 501-242-5332, as shown in Figure 3 below. On or about October 10, 2019, preservation requests were served upon Google to preserve any records they maintain regarding these accounts.

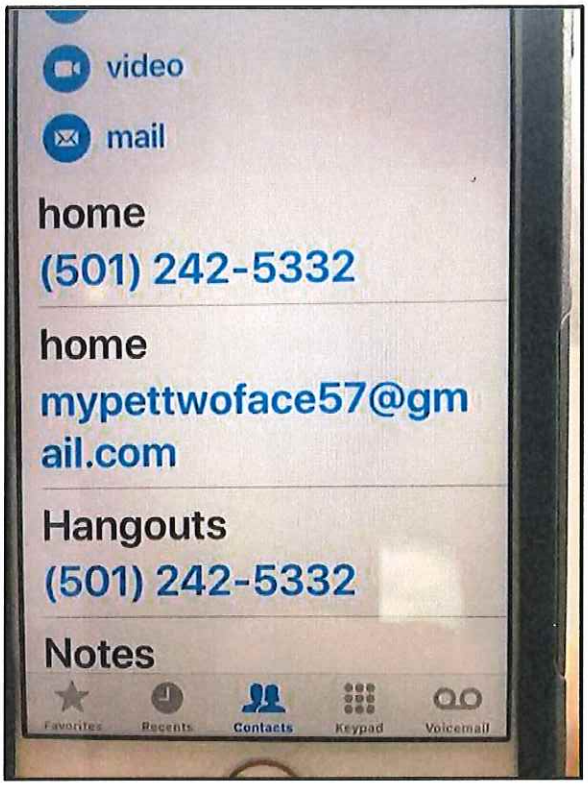

Figure 3

13. With R.A.'s consent, D.A. researched R.A.'s financial matters by reviewing bank statements and speaking with bank employees. R.A. held accounts at Community First Credit Union, Chase Bank, and Nicolet National Bank. According to D.A., R.A.'s bank statements showed that between May 2018 and September 2019, R.A. withdrew at least $142,650 in cash from his own bank accounts. D.A. characterized this activity as entirely unlike R.A.'s decades of frugal and conservative spending habits. D.A.'s summary of R.A.'s cash withdrawals are below:

Ref	Date	Transaction Description	Amount	Financial Institution
a)	7/18/2018	Cash Withdrawal	$ 3,000	Chase Bank
b)	8/9/2018	Cash Withdrawal	$ 20,000	Chase Bank
c)	9/7/2018	Cash Withdrawal	$ 2,000	Chase Bank
d)	10/11/2018	Cash Withdrawal	$ 2,600	Community First Credit Union
e)	10/11/2018	Cash Withdrawal	$ 20,000	Chase Bank
f)	10/15/2018	Cash Withdrawal	$ 30,000	Chase Bank
g)	11/21/2018	Cash Withdrawal	$ 20,000	Nicolet National Bank
h)	11/30/2018	Cash Withdrawal	$ 30,000	Nicolet National Bank
i)	2/22/2019	Cash Withdrawal	$ 3,000	Nicolet National Bank
j)	3/19/2019	Cash Withdrawal	$ 7,000	Nicolet National Bank

k)	4/19/2019	Cash Withdrawal	$	2,500	Nicolet National Bank
l)	5/24/2019	Cash Withdrawal	$	550	Nicolet National Bank
m)	6/24/2019	Cash Withdrawal	$	2,000	Nicolet National Bank
n)	**Total Amount of Cash Withdrawals:**		**$**	**142,650**	

14. D.A. provided your affiant with a Nicolet Bank statement for R.A.'s account ending in 0392 which listed all transactions from November 8, 2018 through May 28, 2019.

15. Among the debit card transactions provided, your affiant saw payments for shipment services through the United States Post Offices at or around the time he withdrew large sums of cash from his bank account. In particular, on November 29, 2018, R.A. withdrew $30,000.00 from his bank account. The next day, he paid the United States Postal Service $7.25 for a flat rate envelope.

16. Figures 4, 5, and 6 as set forth below represent images of documents found by D.A. inside R.A.'s residence:

a. The name of Akinyemi Jonson and 312 Tacoma.

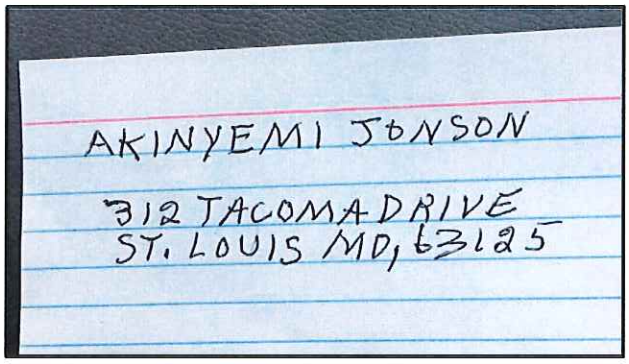

Figure 4

b. The Sender's Copy of United States Priority Mail Express Mail label EK221958946US addressed to Wale Akinmerin at 312 Tacoma dated March 20, 2019

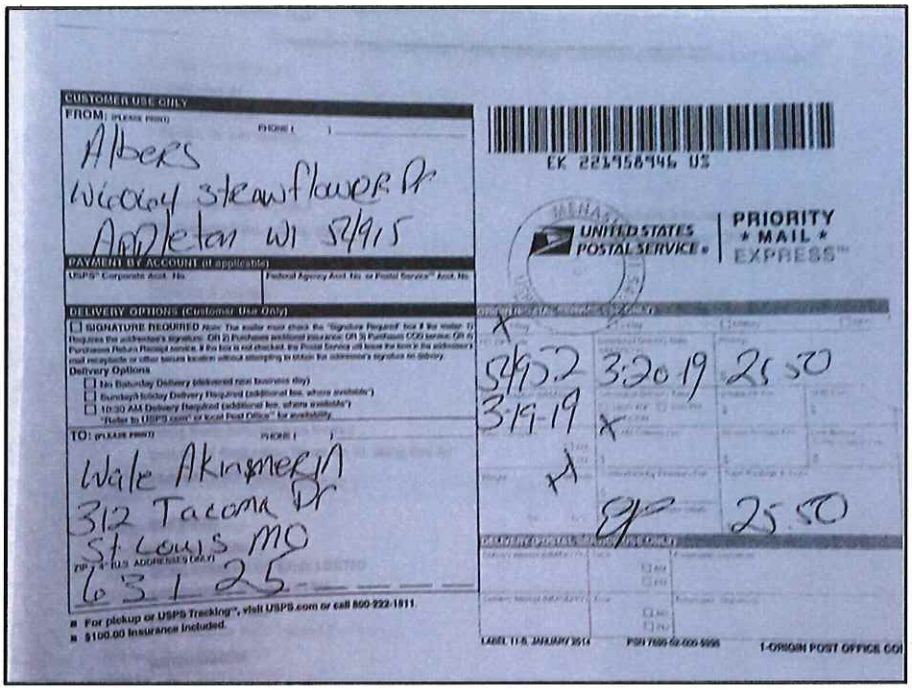

Figure 5

c. A FedEx receipt confirming the scheduled delivery on June 25, 2019 to Wale Akinyemi at 312 Tacoma

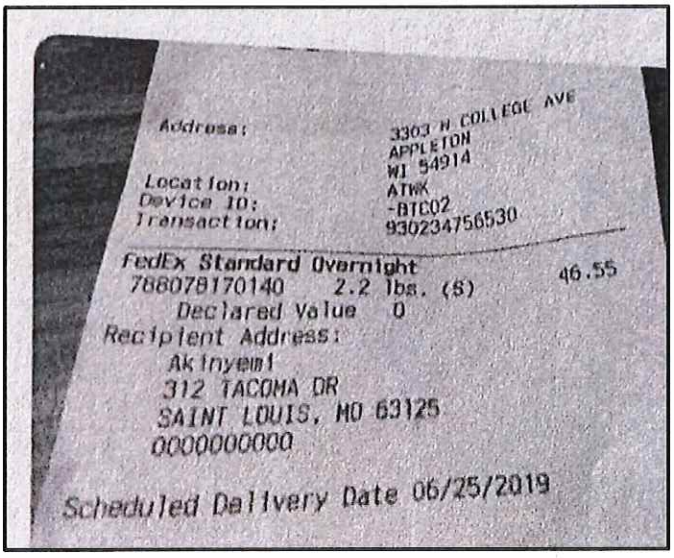

Figure 6

17. Based on the interview of D.A. and the documents provided, your affiant has reason to believe R.A. is a victim of an online romance scam and is being directed to send money under false and/or fraudulent pretenses through the scammer's use of the following:

a. The name Ruth R.O.;

b. The email address MYPETTWOFACE57@GMAIL.COM;

c. The phone number (501) 242-5332; and,

d. The address 312 Tacoma Drive, St. Louis, MO 63125.

IC3 Records

18. The Federal Bureau of Investigation operates a website, the Internet Crime Complaint Center ("IC3"), through which law enforcement can track fraud complaints from victims of internet fraud schemes.

19. Your affiant queried the IC3 for information associated with R.O., **312 Tacoma Drive**, and other keywords.

20. The query resulted in the identification of a complaint filed by "K.H.", on June 6, 2019. K.H., a resident of the Middle District of Pennsylvania, who was over the age of 60, was directed through Google Hangouts to send and/or receive money for an individual with whom K.H. believed she was involved romantically. These individuals included the following:

a. R.A. at his residence in the Eastern District of Wisconsin,

b. Ruth R.O. at 1225 Curtis Lane, in Benton, Arkansas, and

c. J.N. at 151 Grand St, South Amboy, New Jersey.

United States Postal Service Records for 312 Tacoma Drive, St. Louis, MO

21. Your affiant queried U.S. Postal Service ("USPS") records for the U.S. Mail Priority Mail package EK221958946US exhibited as Figure 5. The records showed the package was mailed from the United States Post Office in Menasha, Wisconsin on March 19, 2019, and delivered on March 20, 2019 to 312 Tacoma addressed to Wale Akinmerin.

22. Your affiant queried USPS records for all Priority Mail packages originating near Menasha, Wisconsin with 312 Tacoma destination address, and found the following:

U.S. Mail Label	Date Sent	Date Delivered	Destination Address
9505512491129053052732	2/22/2019	2/25/2019	312 Tacoma Drive, St. Louis, MO 63125

EK221958946US	3/19/2019	3/20/2019	312 Tacoma Drive, St. Louis, MO 63125
EK625398655US	4/19/2019	4/20/2019	312 Tacoma Drive, St. Louis, MO 63125

23. Your affiant compared the package information in the chart above with the cash Withdrawals identified by D.A. in Paragraph 13, and also shown in R.A.'s Nicolet Bank debit card transactions, which showed each of the three packages were mailed to the **312 Tacoma Drive** on the same days that R.A. conducted three large cash Withdrawals.

24. A further query of USPS records revealed that the **312 Tacoma Drive** received at least fifty-eight Priority Mail packages from January 1, 2019 through October 10, 2019. Each of these packages originated form a U.S. Post Office retail counter and/or self-service kiosk and are not associated with online retailers.

25. On October 4, 2019, your affiant reviewed inbound Priority Mail package EJ077131166US. I noted the package was a USPS Priority Mail Express envelope addressed to Tobi Jacobs at **312 Tacoma Drive**. The package was mailed from the Irvine, Kentucky Post Office with a handwritten label indicating the sender was J.S. at an address in Irvine, KY. Your affiant noted characteristics for the mailing by J.S. that are consistent with the characteristics of packages containing money for and at the best of Ruth R.O. sent from R.A.

26. On October 4, 2019, your affiant reviewed inbound Priority Mail package EE301697182US. I noted the package was a USPS Priority Mail Express envelope addressed to Tobi Jacobs at **312 Tacoma Drive**. The package was mailed from the Charleston, South Carolina Post Office with a handwritten label indicating the sender was C.M. at an address in North Charleston, SC. Your affiant noted characteristics for the mailing by C.M. that are consistent with the characteristics of packages containing money for and at the best of Ruth R.O. sent from R.A.

27. On October 7, 2019, your affiant reviewed inbound Priority Mail package EE368638783US. I noted the package was a USPS Priority Mail Express envelope addressed to Yemi Thompson at **312 Tacoma Drive**. The package was mailed from the Oxford, OH Post Office with a handwritten label indicating the sender was L.S. using an address in Oxford, OH 45056. Your affiant noted characteristics for the mailing by L.S. that are consistent with the characteristics of packages containing money for and at the best of R.O. sent from R.A.

United States Postal Service Records for 1545 Hollywood Lane, Florissant, MO

28. In reviewing other financial transactions for R.A., your affiant identified payment by R.A. for the delivery of a package through the United States mails on November 30, 2018 to **1545 Hollywood Lane, Florissant, MO**. USPS records show the debit card transaction was used to pay for postage associated with Priority package 9505512491128334045494 which was delivered on December 3, 2018 to **1545 Hollywood Lane, Florissant, MO 63033**.

29. Your affiant queried USPS records for all Priority Mail packages originating near Menasha, Wisconsin with the **1545 Hollywood Lane, Florissant, MO 63033** destination address and found the following:

U.S. Mail Label	Date Sent	Date Delivered	Destination Address
9505512491128334045494	11/30/2018	12/3/2018	1545 Hollywood Lane Florissant, MO 63033
EK176907760US	11/30/2018	12/1/2018	1545 Hollywood Lane Florissant, MO 63033

30. USPS records show **1545 Hollywood Lane, Florissant, MO 63033** received at least eleven Priority Mail packages from January 1, 2019 through October 10, 2019. Each of these packages originated form a U.S. Post Office retail counter and/or self-service kiosk and are not associated with online retailers.

31. Based on this information, your affiant has reason to believe 1545 Hollywood Lane, Florissant, MO 63033 is also being used to receive funds related to an online romance scam.

Analysis of Priority Mailings to 312 Tacoma Drive and 1545 Hollywood Lane

32. Your affiant queried USPS records for all Priority packages sent to **312 Tacoma Drive, St. Louis, MO 63125** and **1545 Hollywood Lane, Florissant, MO 63033** and grouped them by Originating Post Office. This research identified eleven clusters of addressees which are sending mailings that have characteristics similar to those packages sent by victim R.A. to 312 Tacoma, as shown in the chart below:

Quantity of Packages	Originating Post Office	Victim
17	Charleston, SC	Likely C.M.
13	Winthrop, ME	Unknown at this time.
10	Irvine, KY	Likely J.S.
8	South Amboy, NJ	Likely J.N.

7	Oxford, OH	Likely L.S.
5	Punta Gorda, FL	Unknown at this time.
5	Hamilton, OH	Unknown at this time.
5	Decatur, IN	Unknown at this time.
4	Albuquerque, NM	Unknown at this time.
3	Benton, AR	Likely R.O.
3	Granite City, IL	Unknown at this time.
3	Combined Locks, WI	R.A.
1	Kimberly, WI	R.A.
1	Menasha, WI	R.A.

R.O.

33. In July 2019, FBI interviewed R.O. at an address located in Benton, Arkansas, regarding her involvement in financial transactions related to R.A.

34. R.O. told FBI Agents she met an individual who identified himself as Jerry Guill ("Guill") on an online dating website. Guill claimed to be a gemstone purchaser near Singapore.

35. In 2018, R.O. informed Guill that she was experiencing financial difficulties. As a result, R.O. received various amounts of money, up to and including $20,000.00 from Guill and others on his behalf.

36. According to R.O., she repaid the funds through wire transfers sent through Western Union and MoneyGram to Guill in Nigeria.

Hammed Akande

37. U.S. Citizenship and Immigration Service records reveal that Hammed Akande, hereinafter referred to as "Akande," is a Nigerian National who is a Limited Permanent Resident of the United States.

38. For purposes of his immigration record, Akande reported to the U.S. Citizenship and Immigration Service that he lived with his wife, P.A., and his step-daughter, M.S., at **312 Tacoma Drive**.

39. Missouri Department of Revenue records lists Akande's address on his Missouri driver's license as being **312 Tacoma Drive**.

40. Through further investigation, your affiant learned that Akande's physical address is **1545 Hollywood Lane** with his girlfriend, M.H.

41. USPIS records revealed that, on or about June 28, 2017, Hammed Akande, "Akande," used the address of 312 Tacoma Drive to send a Priority Mail parcel to Peter Otasowie at 1215 Rustic Ave, Rosedale, MD 21237.

42. This parcel was mistakenly delivered to the wrong address. When the unintended recipient opened the parcel they found $9,900 in U.S. currency. Realizing that the package had been delivered to the wrong address, the unintended recipient returned the parcel containing the currency to the Post Office.

43. On or about June 30, 2017, the USPIS was called to investigate because United States currency that has been sent through the mail is associated frequently with drug trafficking organizations. USPIS attempted to identify whether the sender, Akande, or the intended recipient, Peter Otasowie, had any associations with illegal narcotics.

44. The USPIS converted the currency to United States Postal Service Money Orders on or about July 20, 2017.

45. Due to the lack of evidence of criminal drug activity, on or about December 18, 2017, the USPIS in Maryland made the money orders payable to Hammed Akande, and mailed a letter containing the securities to 213 Takoma Drive, St. Louis, MO rather than Hammed Akande's correct mailing address of **312 Tacoma Drive** from the State of Maryland.

46. Because the address was incorrect, on or about December 25, 2017, the United States Postmaster in St. Louis, MO returned the letter containing the money orders to the USPIS in Maryland.

47. On an unknown date after December 25, 2017, the USPIS in Maryland mailed a second package containing the money orders to Akande at his correct mailing address of **312 Tacoma Drive.**

48. On or about July 26, 2018, Akande presented the money orders to a representative of a St. Louis branch of Regions Bank.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

49. As described above and in Attachment B, this application seeks permission to search for records that might be located in the residence of **1545 Hollywood Lane, Florissant, MO 63033**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the

seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

50. *Probable cause.* Your affiant submits that if a computer or storage medium is found on **1545 Hollywood Lane , Florissant, MO 63033**, there is probable cause to believe those records will be stored on that computer or storage medium, for the following reasons:

a. Based on your affiant's knowledge, training, and experience, your affiant knows that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard Drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

51. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe

that this forensic electronic evidence will be on any storage medium in **1545 Hollywood Lane, Florissant, MO 63033** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of

computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, Driveaw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to Driveaw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic

programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. Your affiant knows that when an individual uses a computer to view and save stolen or illegal images and files, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, your affiant believes that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

52. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

53. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant your affiant is applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard Drive to human inspection in order to determine whether it is evidence described by the warrant.

54. Because several people share **1545 Hollywood Lane, Florissant, MO 63033** as a residence, it is possible that **1545 Hollywood Lane, Florissant, MO 63033** will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would also permit the seizure and review of those items.

AFFIANT'S CONCLUSIONS

55. Based on this information, your affiant respectfully submits that there is probable cause to believe that evidence, instrumentalities, contraband, fruits of the crime, or things otherwise criminally possessed, or which is designed or intended for use or which is or has been used as the means of an offense of violations of Title 18, United States Code, Section 1341 (Mail Fraud), Title 18, United States Code, Section 1343 (Wire Fraud), Title 18, United States Code, and/or Section 1028A, (Aggravated Identity Theft), are located at **1545 Hollywood Lane, Florissant,**

MO 63033. By this affidavit and application, this affiant respectfully request that the Court issue a search warrant allowing agents to seize evidence and other information stored on **1545 Hollywood Lane, Florissant, MO 63033**, as described in Attachment A and the items to searched in Attachment B.

REQUEST TO SEAL

56. This affiant respectfully request that the Court order that all documents relating to this application and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation which is neither public nor known to all of the targets of the investigation. Accordingly, this affiant submits that good cause exists to seal these documents so as to not seriously jeopardize the investigation.

Respectfully submitted,

PRD

PETER DYER
Postal Inspector
U.S. Postal Inspection Service

Subscribed and sworn to before me this 30th day of October, 2019.

SHIRLEY P. MENSAH
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

This warrant applies to the property located at 1545 Hollywood, Florissant, Missouri 63033, a single story residential building with brick and wood siding, white trim, and the numbers "1545" displayed diagonally just left of the front door.

The search of this location shall include all rooms, annexes, attics, basements, garages, vehicles, mailboxes, trash containers, debris boxes, storage lockers and areas, cabinets, rooms, covered porches, sheds, and out buildings associated with and under the control of the residents of 1545 Hollywood, Florissant, Missouri 63033.

ATTACHMENT B

Items to be Seized

1. The following materials, which constitute evidence of the commission of a criminal offense or which is contraband, fruits of the crime, or things otherwise criminally possessed, or which is designed or intended for use or which is or has been used as the means of an offense of violations of Title 18 United States Code, Section 1341, Mail Fraud, and or Title 18 United States Code, Section 1343, Wire Fraud, specifically any and all:

a. Records evidencing transactions with delivery services including, but not limited to, U.S. Post Office (USPS), Federal Express (FedEx), United Parcel Services (UPS),

b. Records and other property bearing names and/or addresses,

c. Records evidencing alteration of items to conceal U.S. currency,

d. U.S. currency, Prepaid cards, Gift cards, Virtual currency wallets,

e. Records evidencing transactions with financial institutions including, but not limited to, any bank or credit union, Western Union, MoneyGram, or virtual currency exchanges,

f. Personally identifiable information or records of people other than the residents of the premises to be searched,

g. Records evidencing transactions or communications involving financial fraud schemes,

h. Records evidencing international transactions or communications,

i. Handwritten notes evidencing recording of transactions, communications, names, account numbers, phone numbers, or other identifiers,

j. Computers and storage media used as a means to commit the violations described above,

k. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

l. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "Computer"):

a. evidence of who used, owned, or controlled the Computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, or forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer;

h. evidence of the dates and times the Computer was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the Computer;

j. documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer;

k. records of or information about Internet Protocol addresses used by the Computer;

l. records of or information about the Computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. Contextual information necessary to understand the evidence described in this attachment.

3. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

4. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network equipment used to connect computers to the Internet.

5. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, camera memory cards, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.